Optimal randomness certification in the quantum steering and prepare-and-measure scenarios

2015 New J. Phys. 17 113010

(http://iopscience.iop.org/1367-2630/17/11/113010)

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
19 May 2015

REVISED
2 October 2015

ACCEPTED FOR PUBLICATION
6 October 2015

PUBLISHED
29 October 2015

PAPER

Optimal randomness certification in the quantum steering and prepare-and-measure scenarios

Elsa Passaro[1,4], **Daniel Cavalcanti**[1], **Paul Skrzypczyk**[1,2] **and Antonio Acín**[1,3]

[1] ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, E-08860 Castelldefels (Barcelona), Spain
[2] H. H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol, BS8 1TL, UK
[3] ICREA-Institució Catalana de Recerca i Estudis Avançats, Lluis Companys 23, E-08010 Barcelona, Spain
[4] Author to whom any correspondence should be addressed.

E-mail: elsa.passaro@icfo.es

Keywords: randomness certification, quantum steering, prepare-and-measure

Abstract

Quantum mechanics predicts the existence of intrinsically random processes. Contrary to classical randomness, this lack of predictability can not be attributed to ignorance or lack of control. Here we find the optimal method to quantify the amount of local or global randomness that can be extracted in two scenarios: (i) the quantum steering scenario, where two parties measure a bipartite system in an unknown state but one of them does not trust his measurement apparatus, and (ii) the prepare-and-measure scenario, where additionally the quantum state is known. We use our methods to compute the maximal amount of local and global randomness that can be certified by measuring systems subject to noise and losses and show that local randomness can be certified from a single measurement if and only if the detectors used in the test have detection efficiency higher than 50%.

One of the most distinct features of quantum mechanics is its intrinsically random character. While in classical mechanics lack of predictability can always be associated to ignorance or lack of control of the probed systems, the rules of quantum physics say that one can not predict the outcome of a measurement even if all the variables of a system are known. This inherent unpredictability has been exploited in different applications such as quantum random number generation [1] and quantum key distribution [2].

Recent results have shown that the randomness observed in quantum mechanics can be certified even without relying on any modelling of the quantum devices used for the generation of the random data. In fact, by analysing the data obtained in experiments involving local measurements on bipartite entangled systems one can prove that no one could have predicted this data in advance whenever a Bell inequality violation is observed [3, 4]. This is called device-independent (DI) randomness certification [5, 6]. The DI approach has the practical advantage that it does not rely on the exact description of the experimental set-up. This is crucial when implementing cryptographic protocols as an adversary can use a mismatch between the theoretical description and the actual implementation of the set-up to fake its performance [7–9]. However, DI protocols require low levels of noise [4], which make them very demanding experimentally.

An intermediate scenario is that of quantum steering [10, 11]. It refers to the case where two parties, say Alice and Bob, apply local measurements on an unknown bipartite system. While one of them, Bob, has complete knowledge of his measurement apparatuses, Alice does not, and treats her measuring device as a black box with classical inputs and outputs. Quantum steering has been receiving lot of attention recently due to the fact that it allows for entanglement detection which is more robust to noise and experimental imperfections than Bell nonlocality [11, 12]. Moreover, quantum steering was shown to be useful for one-sided device independent quantum key distribution (1SDIQKD) [13] and randomness certification [14]. Several experimental groups have recently observed steering, including in continuous-variable systems [15, 16], using Bell local states [17], using inefficient detectors [18–20], asymmetric states [21], and multipartite systems [22–24].

The main result of our paper is a general and optimal method to quantify the amount of local or global randomness that can be certified from a single measurement in a steering experiment. We use this method to

show that local randomness can be certified provided that the detectors used have efficiency higher than 50%. Our method can be seen as the analogue of the approach of [25, 26] from the fully DI scenario applied to the steering scenario. We compare the results obtained there to those obtained here, in terms of the amount of randomness that can be obtained by measuring systems subjected to white noise, and find substantial benefits can be obtained in the present setting. As a by-product, we also show that the amount of randomness certified in [14] from the two-qubit Werner state is optimal.

We furthermore show that the results can be easily extended beyond the steering scenario, to the prepare-and-measure scenario, where the state is also trusted, so that only Alice's measuring device is untrusted. In this case we show that even noisy states can perform very well for randomness certification.

Finally, we give a method to find the best measurements which obtain the most randomness from any fixed state. Using insight from this method, we show analytically that all pure partially entangled states lead to maximal randomness certification using only two fixed measurements.

There are several motivations to quantify the amount of randomness in the steering scenario. From a fundamental point of view, it is important to understand how much randomness can be maintained if we give up partial information about the specific description of the systems [14, 27, 28]. From a practical point of view, the amount of randomness obtained in the steering scenario gives an upper bound to what Alice and Bob would obtain in a fully DI setting, regardless of the number of measurements Bob would apply. Furthermore, it is a scenario that appears naturally in some asymmetric applications. For instance the present results give a way of quantifying the amount of randomness in remote untrusted stations. This is relevant, for instance, when the provider of a quantum-random-number generator wants to remotely check if the devices they provided are still functioning properly.

1. Steering and randomness

The scenario we treat in this work is the following [11]: two parties, Alice and Bob, are located in distant laboratories and receive a bipartite system from a source. One of the two parties, say Alice, does not trust her measuring devices, which are treated as 'black boxes'. She can, nevertheless, choose which measurement to perform, which she labels by $x \in \{0, \ldots, m_A - 1\}$, each of which provides an outcomes, which she labels $a \in \{0, \ldots, n_A - 1\}$. The other party, Bob, has complete knowledge of his device, which allows him to perform quantum state tomography on his part of the system, and thus to obtain a complete description of his subsystem (see figure 1(a)). The states reconstructed by Bob will usually depend on Alice's input and output as $\rho_{a|x} = \mathrm{Tr}_A[(M_{a|x} \otimes \mathbb{1}_B)\rho_{AB}]/P(a|x)$, where ρ_{AB} is the unknown state shared with Alice, $P(a|x)$ is the probability that Alice observes outcome a given she chose x, and $M_{a|x}$ is the corresponding (unknown) element of Alice's measurement. The set of unnormalized states $\sigma_{a|x} = \mathrm{Tr}_A[(M_{a|x} \otimes \mathbb{1}_B)\rho_{AB}] = \rho_{a|x}P(a|x)$ is called an *assemblage* and can be completely determined by Bob through tomographic measurements.

As noticed in [11], Bob can determine if ρ_{AB} is entangled by looking at the form of the assemblage $\{\sigma_{a|x}\}_{a,x}$. This is because separable states can only lead to assemblages with the specific form

$$\sigma_{a|x} = \sum_{\lambda} q(\lambda) P(a|x, \lambda)\sigma_{\lambda}, \tag{1}$$

where λ is a hidden variable distributed according to $q(\lambda)$, which determines both Alice's response $P(a|x, \lambda)$, and the states sent to Bob, σ_{λ}. Assemblages of this form are said to have a local hidden state model. Any assemblage which does not have this form can be detected through the violation of a steering inequality [29] (similar to a Bell inequality or an entanglement witness) or a simple semi-definite program [30].

It turns out that the confirmation of steering not only guarantees that the shared state is entangled, but also that Alice is performing incompatible measurements [31, 32]. It is thus very intuitive to expect a relation between steering and randomness: first, the correlations (entanglement) shared between Alice and Bob allows Bob to certify steering, and consequently the incompatibility of Alice's measurements. Second, since Alice's measurements are incompatible not all the outcomes she receives are predictable, and thus random.

2. Local randomness certification

In order to certify the local randomness of Alice's outcomes we work in the adversarial scenario, where a potential eavesdropper, Eve, wants to predict them. This framework is relevant for cryptographic tasks, namely ISDIQKD. In the most general case, we do not make any assumption on Alice's measurement device, so that it could even have been provided by Eve. We also consider that the state ρ_{AB} is the reduced state of a tripartite entangled state ρ_{ABE} shared by Alice, Bob and Eve, i.e. $\rho_{AB} = \mathrm{Tr}_E[\rho_{ABE}]$. Hence, by applying measurements to her subsystem Eve can in principle obtain information about Alice's outcome.

In this section we will focus on the case where Alice and Bob want to extract randomness from the outcomes of a single given measurement of Alice, let us say $x^* \in \{0, \ldots, m_A - 1\}$. The motivation for considering this case is that it is the relevant one from the perspective of 1SDIQKD. We assume that the runs of the experiment are independent and identically distributed with respect to Eve's strategy[5]. We consider the case where Eve also knows from which measurement x^* Alice is going to extract randomness, so she can optimize her attack to obtain information about this measurement setting. The figure of merit we use to evaluate the amount of randomness in Alice's outcomes is the probability that Eve can correctly guess the outcome a of the measurement x^* of Alice. This quantity, denoted by $P_{\text{guess}}(x^*)$, is given by the probability that Eve's guess e is equal to the outcome a that Alice obtained, whenever Alice performs the specific measurement $x = x^*$:

$$P_{\text{guess}}\left(x^*\right) = \sum_e P_{\text{A}}\left(a = e \,\middle|\, x^*\right) P_{\text{E}}\left(e \,\middle|\, a = e,\, x = x^*\right). \tag{2}$$

Applying Bayes theorem, this is equivalent to $P_{\text{guess}}(x^*) = \sum_e P_{\text{AE}}(a = e,\, e|x = x^*)$, i.e. equal to the joint probability that Alice and Eve give the same outcome whenever Alice measures $x = x^*$. Randomness is certified whenever the guessing probability is strictly less than 1, in which case Eve can not predict Alice's outcome with certainty.

After Alice and Eve have applied their measurements the assemblage prepared will be

$$\sigma^e_{a|x} = \text{Tr}_{\text{AE}}\left[\left(M_{a|x} \otimes \mathbb{1}_{\text{B}} \otimes M_e\right) \rho_{\text{ABE}}\right], \tag{3}$$

where M_e is the element of Eve's (optimal) measurement which yields outcome $e \in \{0, \ldots, n_{\text{A}} - 1\}$. However, since Alice and Bob do not have access to Eve's outcomes the assemblage they will reconstruct will be given by

$$\sigma^{\text{obs}}_{a|x} = \sum_e \sigma^e_{a|x}. \tag{4}$$

In order to compute the optimal strategy for Eve we need to maximize her guessing probability (for a given input x^* of Alice), over all strategies. Naively, this would appear to constitute optimizing the triple $\{\rho_{\text{ABE}}, M_{a|x}, M_e\}$, of state, measurements for Alice, and measurement for Eve, a nonlinear optimization problem. However, just as in the DI case [25, 26], we can instead replace this by an equivalent linear optimization over all physical assemblages $\{\sigma^e_{a|x}\}_{a,e,x}$ that are compatible with the no-signalling principle and the observed assemblage $\{\sigma^{\text{obs}}_{a|x}\}_{a,x}$. More precisely, the maximization problem can be formulated as the following semidefinite programme (SDP) [33]:

$$\begin{aligned}
\max_{\left\{\sigma^e_{a|x}\right\}_{a,e,x}} \quad & P_{\text{guess}}\left(x^*\right) = \sum_e \text{Tr}\left(\sigma^e_{a=e|x^*}\right) & \\
\text{subject to} \quad & \sum_e \sigma^e_{a|x} = \sigma^{\text{obs}}_{a|x} & \forall\ a,\, x \\
& \sum_a \sigma^e_{a|x} = \sum_a \sigma^e_{a|x'} & \forall\ e,\, x \neq x' \\
& \sigma^e_{a|x} \succcurlyeq 0 & \forall\ a,\, x,\, e.
\end{aligned} \tag{5}$$

In the objective function we used $P_{\text{E}}(e) P_{\text{A}}(a|x,\, e) = P(ae|x) = \text{Tr}[\sigma^e_{a|x}]$ to re-express $P_{\text{guess}}(x^*)$. The first constraint assures that the decomposition for Eve is compatible with the assemblage Alice and Bob observe. The second constraint is the non-signalling condition—i.e. Alice cannot signal to Bob and to Eve. The last one is the requirement for every $\sigma^e_{a|x}$ to be a valid (unnormalized) quantum state. We defer to the appendix the full proof that this optimization problem is equivalent to optimizing over states and measurements, which follows from the Gisin–Hughston–Jozsa–Wootters (GHJW) theorem [34] (which shows that all bipartite no-signalling assemblages have quantum realizations), combined with the fact that Eve, making only one measurement, also cannot signal.

Notice that the SDP (5) can be seen as the steering analogue of the SDP provided in [25, 26] which bounds the amount of randomness given an observed nonlocal probability distribution $P_{\text{obs}}(ab|xy)$. As mentioned before, the SDP (5) provides an upper bound on the amount of randomness (i.e. a lower bound on the P_{guess}) that can be found using the SDP of [25, 26]. This follows because (5) does not allow Eve to attack the measurements of Bob. Thus, our SDP bounds the maximal amount of randomness that could be obtained if Bob were to perform any number of measurements (that Eve can attack) and compute the randomness based on the obtained probability distribution. The number of random bits is quantified by the min-entropy $H_{\min}(A|X) = -\log_2 P^*_{\text{guess}}(x^*)$, where $P^*_{\text{guess}}(x^*)$ is the result of the maximization (5).

In figure 2 we plot the amount of randomness certified in the case that Alice applies two mutually unbiased Pauli spin measurements on a two-qubit Werner state $\rho_{\text{AB}} = \nu\, |\Phi_+\rangle\langle\Phi_+| + (1 - \nu)\mathbb{1}/4$, where

[5] We note that once independence is assumed, it is without loss of generality to assume the pairs identical.

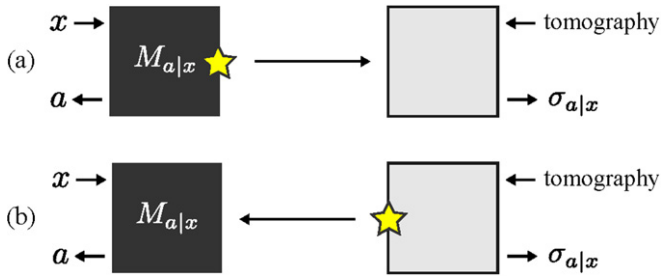

Figure 1. Setup for randomness certification in the quantum steering and prepare-and-measure scenarios. (a) Steering scenario: Alice and Bob measure an unknown bipartite system delivered by an untrusted source. Alice treats her measurement device as a black box with inputs $x \in \{0, \ldots, m_A - 1\}$ and outputs $a \in \{0, \ldots, n_A - 1\}$ and Bob performs tomography on his subsystem. (b) Prepare-and-measure scenario: similar to the previous scenario, but now Bob holds the source and then knows the bipartite state ρ_{AB}.

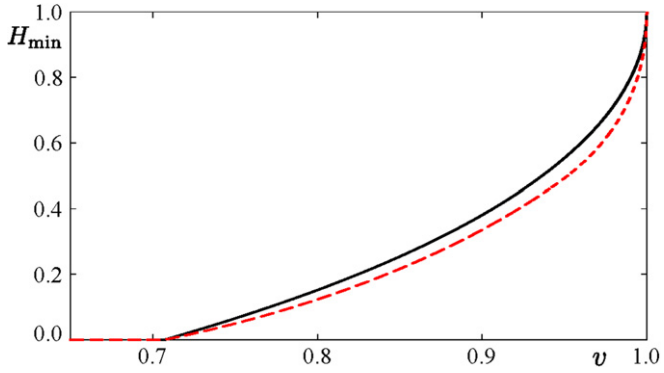

Figure 2. Random bits certified $H_{\min}$ versus the visibility v of the two-qubit Werner state. We compare the randomness obtained with our method in the steering scenario (solid line) with the fully device-independent case as in [25] (dashed line).

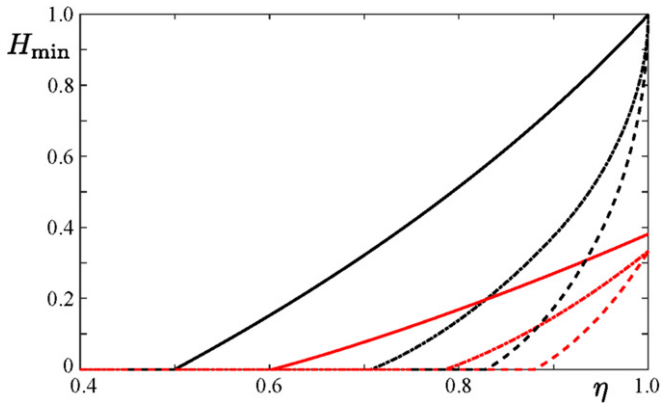

Figure 3. Random bits certified $H_{\min}$ versus the detection efficiency η for the two-qubit Werner state. Black lines: $v = 1$; red lines: $v = 0.9$. Solid lines: our steering method; dotted-dashed lines: DI method in the case where Bob's detection efficiency is 1; dashed lines: DI method where both Alice and Bob's detectors have efficiency η.

$|\Phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, and compare it with the amount of randomness obtained in the case Bob also treats his measuring device as a black box (i.e. the fully DI case). In both cases randomness can be certified as long as $v > 1/\sqrt{2}$, which is the critical amount of noise for demonstrating either steering or nonlocality with only two measurements [35]. All numerical SDP calculations were performed using the CVX package for MATLAB [36], along with the library QETLAB [37].

In figure 3 we also compute the amount of randomness that can be obtained by measuring the same spin measurements with detection efficiency η (for visibility $v = 1$ and $v = 0.9$), again comparing to the case where Bob treats his measuring device as a black box. That is, (for steering) instead of ideal measurements, with

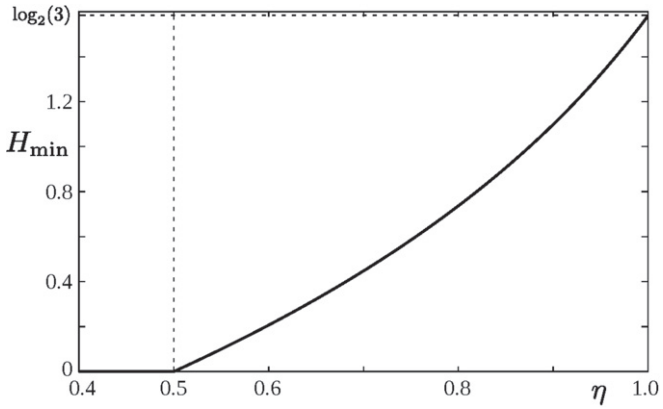

Figure 4. Random bits certified $H_{\min}$ versus the detection efficiency η for the two-qutrit maximally entangled state $|\Phi_+^{(3)}\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$.

elements $M_{a|x}$, we consider inefficient measurements $M_{a|x}^{(\eta)}$, with one additional outcome $a = \varnothing$, given by

$$M_{a|x}^{(\eta)} = \begin{cases} \eta M_{a|x}, & a \neq \varnothing \\ (1-\eta)\mathbb{1}, & a = \varnothing \end{cases} \tag{6}$$

(the measurements of Bob are similarly made inefficient in the nonlocality scenario).

In this case, two comparisons are made: (i) the case where Bob's detection efficiency is 1; and (ii) where Bob also has detection efficiency η. As one can see, for $v = 1$ in the steering scenario randomness can be certified whenever the detection efficiency is higher than 50%, matching the threshold below which no randomness can be obtained [38]. Moreover, we see that due to the much larger detection efficiencies needed to violate the CHSH inequality (82.8%) and for the DI case where Bob's measuring device is perfectly efficient (70.7%), the steering scenario offers a significant advantage when using the maximally entangled state over the nonlocality scenario, for the entire range of visibility which is experimentally significant (i.e. for $v = 0.9$ and above).

Finally, in figure 4 we plot the number of random bits certified in the case that Alice performs measurements in four mutually unbiased bases on her half of the entangled two-qutrit state $(|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$ in the presence of losses. Again, we see that whenever the detection efficiency is above 50% Alice is able to certify local randomness. Moreover, for efficiency $\eta = 1$ she certifies $H_{\min} = \log_2 3$ bits of randomness.

3. Global randomness certification

In the steering scenario one can also consider global randomness extraction from both the untrusted and trusted devices. Indeed, even though Bob trusts his devices, and knows which measurement he performs, there is still an optimal state that Eve can distribute which allows her to predict the outcome of Bob's measurement. This is because although Eve is not able to change the measurements performed by Bob, nor his reduced state, she still has additional classical side information that she can use to help her in guessing the result of Bob (since she holds the source).

Consider that, additionally to Alice's measurement $x = x^*$, Eve wants to guess the outcomes of a measurement M_b performed by Bob. Eve now has a pair of guesses (e, e'), which will be her guess for the pair (a, b). She will thus perform a measurement with elements $M_{ee'}$ on her share of the state, which after Alice also measures will lead to the assemblage for Bob $\sigma_{a|x}^{ee'} = \mathrm{tr}_{\mathrm{AE}}[(M_{a|x} \otimes \mathbb{1}_{\mathrm{B}} \otimes M_{ee'})\rho_{\mathrm{ABE}}]$. Similarly to the case of local randomness, the global guessing probability P_{g} can straightforwardly be shown to be the solution to the following SDP

$$\begin{aligned} P_{\mathrm{g}} = \max & \sum_{ee'} \mathrm{Tr}\left[M_{b=e'} \sigma_{a=e|x^*}^{ee'} \right] \\ \text{s.t.} \quad & \sum_{ee'} \sigma_{a|x}^{ee'} = \sigma_{a|x}^{\mathrm{obs}}, && \forall\ a, x \\ & \sum_{a} \sigma_{a|x}^{ee'} = \sum_{a} \sigma_{a|x'}^{ee'}, && \forall\ x \neq x', a, e, e' \\ & \sigma_{a|x}^{ee'} \succcurlyeq 0, && \forall\ a, x, e, e'. \end{aligned} \tag{7}$$

We again require consistency with the observed assemblage $\sigma_{a|x}^{\mathrm{obs}}$, and demand positivity and no-signalling.

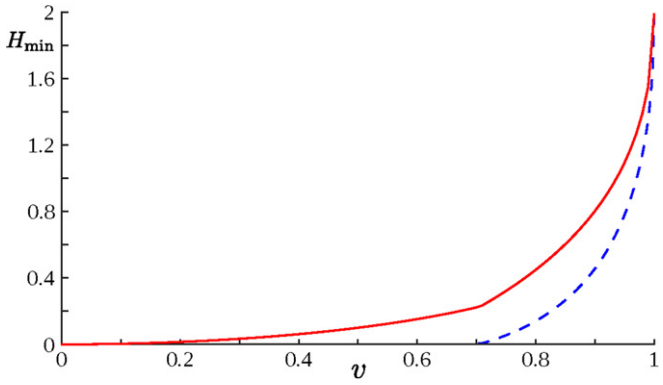

Figure 5. Global randomness obtained by measuring a two-qubit Werner state (with noise v), with X and Z measurements for Alice, and X measurement for Bob, computed using equation (7) (solid curve). As a matter of comparison we also plot the amount of global randomness obtained in the device-independent scenario, using the methods of [25, 26] (dashed curve).

We computed the global randomness which can be certified without losses assuming X and Z measurements for Alice, and an X measurement for Bob, on two-qubit Werner states. The results can be seen in figure 5, alongside the corresponding curve calculated using the method of [25, 26] for the nonlocality scenario. As a result, we observe that the lower bound on the amount of global randomness that can be extracted in the steering scenario presented in [14] is tight.

4. Prepare-and-measure scenario

Up to now we have considered the steering scenario, where Alice and Bob receive an unknown state ρ_{AB} from an untrusted source. It turns out that the results on local randomness straightforwardly apply to the case where Bob prepares a known state and sends half of it to Alice (see figure 1(b)). In this case, since the global state ρ_{AB} is known, the assemblages reconstructed by Bob have to come from unknown measurements on this state, i.e. $\sigma_{a|x} = \sum_e \mathrm{Tr}_{\mathrm{A}}[(M^e_{a|x} \otimes \mathbb{1}_{\mathrm{B}})\rho_{\mathrm{AB}}]$. Thus the SDP (5) can be replaced by

$$\begin{aligned}
\max_{\{M^e_{a|x}\}_{a,e,x}} \quad & P_{\mathrm{guess}}(x^*) = \sum_e \mathrm{Tr}\left[\left(M^e_{a=e|x^*} \otimes \mathbb{1}_{\mathrm{B}}\right)\rho_{\mathrm{AB}}\right] \\
\text{subject to} \quad & \sum_e \mathrm{Tr}_{\mathrm{A}}\left[\left(M^e_{a|x} \otimes \mathbb{1}_{\mathrm{B}}\right)\rho_{\mathrm{AB}}\right] = \sigma^{\mathrm{obs}}_{a|x} \qquad \forall\ a, x \\
& \sum_a M^e_{a|x} = \sum_a M^e_{a|x'} \qquad \forall\ x' \neq x,\ e \\
& \sum_{a,e} M^e_{a|x} = \mathbb{1} \qquad \forall\ x \\
& M^e_{a|x} \succcurlyeq 0 \qquad \forall\ a, x, e. \qquad (8)
\end{aligned}$$

This SDP can be understood as the maximization of Eve's guessing probability over all possible POVM measurements (where the outcome e goes to Eve and the outcome a goes to Alice), with Eve oblivious of x, that can be applied to the state ρ_{AB}, given the observation of the assemblage $\{\sigma^{\mathrm{obs}}_{a|x}\}_{a,x}$. A derivation of this SDP can be found in appendix B. We note that this scenario can also be thought of as the 'time-like steering' scenario introduced in [39].

We used the above program to calculate the amount of randomness that can be obtained from the two qubit Werner state, and from the isotropic two-qutrit state $\rho_{\mathrm{AB}} = v\,|\Phi^{(3)}_+\rangle\langle\Phi^{(3)}_+| + (1-v)\mathbb{1}/9$, where $|\Phi^{(3)}_+\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$. In both cases we consider that Alice performs two mutually unbiased measurements (Pauli X and Z for qubits, and their generalization for qutrits).

For the case of no-losses, we observe that the amount of randomness that can be extracted is *independent of the visibility* v, and equal to 1 bit and 1 trit $= \log_2(3)$ bits respectively[6]. This coincides with the amount which is obtained in the steering scenario for $v = 1$, i.e. the ideal case. This demonstrates that if knowledge of the state is assumed, then the lack of visibility cannot be used by Eve to guess the outcomes of Alice's measurements.

[6] More precisely, for all $v \geqslant 0.05$ we observed numerically that $P_{\mathrm{g}} \leqslant 0.339$.

Turning to the case of losses, consistent with the above, we observe that, independent of the visibility, the dependence of the randomness on the loss coincides with that found in the steering scenario for perfect visibility. That is, the solid black curves in figures 3 and 4 are obtained, for any fixed value of the visibility v.

This shows that the prepare-and-measure scenario greatly improves over the steering scenario when considering lack of visibility (i.e. noise) on the state.

5. Improving the randomness extraction

The SDP (5) provides a way of quantifying the randomness in Alice's outcomes given the observation of a given assemblage. A natural question is, given a fixed state distributed between Alice and Bob and a fixed number of measurements for Alice, what is the best scheme they can implement (i.e. the best choice of measurements) which allows for the certification of the most randomness.

Here we propose a numerical see-saw method that, starting from an initial amount of certified randomness, seeks for measurement schemes that lead to higher randomness certification. We focus on the case of local randomness. A similar scheme can also be implemented for global randomness.

Every SDP has a dual program, also an SDP, that can be obtained through the theory of Lagrange multipliers [33]. The dual of (5) is equivalent to

$$\begin{aligned} \min_{\{F_{a|x}\}_{a,x}} \quad & \sum_{a,x} \mathrm{Tr}\left(F_{a|x}\,\sigma^{\mathrm{obs}}_{a|x}\right) \\ \text{subject to} \quad & \mathrm{Tr}\left[\sigma_{a'|x^*}\right] \leqslant \sum_{a,x} \mathrm{Tr}\left(F_{a|x}\sigma_{a|x}\right) \qquad \forall\ a',\ \sigma_{a|x}, \end{aligned} \tag{9}$$

where in the constraint, $\forall\ \sigma_{a|x}$ should be understood as for all non-signalling assemblages, i.e. those satisfying $\sum_a \sigma_{a|x} = \sum_a \sigma_{a|x'}$ for all[7] $x' \neq x$. Since strong duality holds, the optimal value of this optimization problem is equal to the optimal value of (5), i.e. $P^*_{\mathrm{guess}}(x^*) = \sum_{a,x} \mathrm{Tr}(F^*_{a|x}\,\sigma^{\mathrm{obs}}_{a|x})$. Moreover, it outputs the coefficients $F^*_{a|x}$ of the optimal steering inequality that gives the tight upper bound on $P^*_{\mathrm{guess}}(x^*)$.

Once we have solved the dual problem (9) we can run a second SDP that optimizes the violation of the steering inequality $\sum_{a,x} \mathrm{Tr}(F^*_{a|x}\,\sigma_{a|x})$ over Alice's measurements $\{M_{a|x}\}_{ax}$:

$$\begin{aligned} \min_{\{M_{a|x}\}_{ax}} \quad & \sum_{ax} \mathrm{Tr}\left[\left(M_{a|x} \otimes F_{a|x}\right)\rho_{AB}\right] \\ \text{subject to} \quad & \sum_a M_{a|x} = \mathbb{1} \qquad \forall\ x \\ & M_{a|x} \succcurlyeq 0 \qquad \forall\ a,\ x. \end{aligned} \tag{10}$$

The solution of this optimization problem provides the measurements for Alice that allow for the certification of the most randomness using the steering inequality provided by the first SDP.

At this point, one can perform a see-saw iteration of the two SDPs in order to obtain the maximal randomness that can be certified from a given state, along with the optimal steering inequality and measurements $M_{a|x}$. For every given initial state, the SDP (5) (and its dual (9)) gives the best inequality to certify randomness from an assemblage, while the SDP (10) gives the best set of measurements—and therefore the best assemblage—for a given steering inequality.

In figure 6 we plot the result of this see-saw iteration, starting from two randomly chosen projective measurements, for $\eta = 1$ and $\eta = 0.9$, for the two-qubit partially entangled state $|\psi\rangle = \cos\theta\ |00\rangle + \sin\theta\ |11\rangle$. When there are no losses, one bit of randomness is already known to be possible from any partially entangled state in the fully DI scenario [40]. Since this scenario is more demanding, it implies one bit can also be obtained from any partially entangled state of two qubits in the steering scenario. If the method works it should be able to reproduce this result. As can be seen, 1 bit of randomness is indeed found, thus demonstrating the utility of the method.

Further exploration showed numerically that the measurements which achieve 1 bit of randomness from any partially entangled state can always be taken to be X and Z measurements for Alice (with the randomness obtained from the X measurement)[8].

In the appendix we show that this numerical evidence can in fact be turned into an analytic construction, which proves that 1 bit can be obtained from any partially entangled state of two qubits (which is notably

[7] As written, this problem is not in the form of SDP. In appendix C we derive the dual SDP and show its equivalence to (9), which is easier to interpret.

[8] We do not present the form of the optimal steering inequalities for partially entangled states, since we did not find any general structure which makes knowing their form useful.

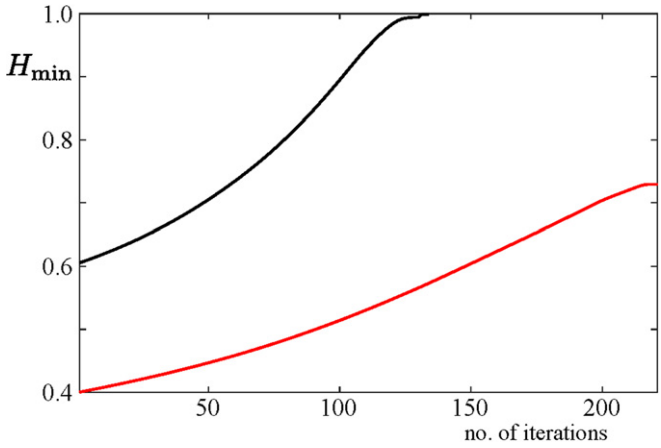

Figure 6. Plot of the random bits certified versus the number of steps of the see-saw iteration for a two-qubit partially entangled state $|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$ with $\theta = \pi/7$ and starting with random measurements with $\eta = 1$ (black curve) and $\eta = 0.9$ (red curve).

completely different to the approach used in [40] for nonlocality). Moreover, the construction generalizes to qudits in a straightforward manner, showing that 1 dit of randomness can be obtained by performing two generalized Pauli measurements on any Schmidt-rank d state. This is contrary to the fully DI case, where it is only known how to extract 1 bit from any pure partially entangled state.

6. Conclusions

We have presented a method that certifies the optimal amount of local or global randomness that can be extracted in a steering experiment. We also considered the case where the source is trusted (prepare-and-measure scenario). Our method relies on optimization techniques that quantify the amount of certified randomness and provide the optimal steering inequality for randomness certification. Applying this method to realistic implementations—i.e. in presence of noise and losses—we have shown that a detection efficiency above 50% is sufficient to have reliable local randomness certification in the steering scenario. This result is also valid for DI randomness certification and, in general, in scenarios with lower levels of trust.

Finally, we have introduced a method which produces, for any given initial state, the optimal measurements which in turn give the optimal assemblage from which maximal randomness can be certified. Using this method as a starting point, we have shown analytically that 1 dit of randomness can be obtained from any pure entangled Schmidt-rank d state.

Since local randomness certification is of fundamental importance for 1SDI and DI QKD, the results presented here have a natural application in cryptographic protocols.

Acknowledgments

We thank R Rabelo for discussions on randomness in an early stage of this project. This work was supported by the Beatriu de Pinós fellowship (BP-DGR 2013),the Marie Curie COFUND action through the ICFOnest program, the ERC CoG QITBOX, the ERC AdG NLST, the EU project SIQS, the Spanish project FOQUS, the Generalitat de Catalunya (SGR875) and the John Templeton Foundation. EP acknowledges the Max Planck Institute for Quantum Optics for hospitality.

Appendix A. Obtaining the SDP for the guessing probability

In this appendix we will show how to arrive at the SDP (5) for Eve's guessing probability.

The most general attack that Eve can implement in the case that she is interested in guessing the result of a single measurement ($x = x^*$) Alice, is to distribute a state ρ_{ABE} to Alice and Bob (keeping a part for herself) on which she will perform a measurement with POVM elements M_e, for $e = 0, \ldots, m_{\mathrm{A}} - 1$, and distribute to Alice a set of measuring devices which implement the POVMs with elements $M_{a|x}$, for $x = 0, \ldots, n_{\mathrm{A}} - 1$ and $a = 0, \ldots, m_{\mathrm{A}} - 1$. When Eve obtains outcome e from her measurement she will give this as her guess for the outcome of Alice. Thus, the guessing probability of Eve is given by

$$P_{\text{guess}}\left(x^*\right) = \sum_e \text{Tr}\left[\left(M_{a=e|x^*} \otimes M_e\right)\rho_{\text{AE}}\right]. \tag{A.1}$$

Alice and Bob can however determine the assemblage $\sigma^{\text{obs}}_{a|x}$ that they hold, (i.e. the set of conditional states prepared for Bob, along with the corresponding probabilities). Thus the optimization problem we need to solve is given by

$$\begin{aligned}\max_{\rho_{\text{ABE}},\{M_{a|x}\}_{a,x},\{M_e\}_e} \quad & \sum_e \text{Tr}\left[\left(M_{a=e|x^*} \otimes M_e\right)\rho_{\text{AE}}\right] \\ \text{subject to} \quad & \text{Tr}_{\text{A}}\left[\left(M_{a|x} \otimes \mathbb{1}_{\text{B}}\right)\rho_{\text{AB}}\right] = \sigma^{\text{obs}}_{a|x},\ \forall\ a, x \\ & \rho_{\text{ABE}} \succcurlyeq 0, \quad \text{Tr}\,\rho_{\text{ABE}} = 1 \\ & M_{a|x} \succcurlyeq 0,\ \forall\ a, x \quad \sum_a M_{a|x} = \mathbb{1},\ \forall\ x \\ & M_e \succcurlyeq 0,\ \forall\ e \quad \sum_e M_e = \mathbb{1}.\end{aligned} \tag{A.2}$$

Here, the first constraint is the consistency with the observed assemblage, the second constraints demand that ρ_{ABE} is a valid quantum state and the third and fourth constraints that the measurements $M_{a|x}$ and M_e are valid POVMs.

Defining now the joint assemblage for Alice, Bob and Eve

$$\sigma^e_{a|x} = \text{Tr}_{\text{AE}}\left[\left(M_{a|x} \otimes \mathbb{1}_{\text{B}} \otimes M_e\right)\rho_{\text{ABE}}\right], \tag{A.3}$$

it is straightforward to see that all of the constraints appearing in (5) are satisfied whenever the constraints in (A.2) are satisfied, and that the objective functions match. Thus it is straightforward to see that the optimization problem (5) is at least a relaxation of (A.2). What we will show now is that they are in fact equivalent optimization problems by showing that any solution to (5) also implies a solution to (A.2).

First of all, consider an assemblage $\sigma^e_{a|x}$ satisfying all of the constraints in (5). For a fixed e, we can define[9] $P_{\text{E}}(e) = \sum_a \text{Tr}\,\sigma^e_{a|x}$, and $\tilde{\sigma}^e_{a|x} = \sigma^e_{a|x}/P_{\text{E}}(e)$. This has the following properties

$$\sum_a \tilde{\sigma}^e_{a|x} = \sum_a \tilde{\sigma}^e_{a|x'} \quad \forall\ e, x \neq x', \qquad \text{Tr}\sum_a \tilde{\sigma}^e_{a|x} = 1 \quad \forall\ e \tag{A.4}$$

which show that for each e, $\tilde{\sigma}^e_{a|x}$ is a valid assemblage [30]. From the GHJW theorem [34] it therefore follows that there is a quantum state ρ^e_{AB} and POVM elements $M^e_{a|x}$ such that

$$\text{Tr}_{\text{A}}\left[\left(M^e_{a|x} \otimes \mathbb{1}_{\text{B}}\right)\rho^e_{\text{AB}}\right] = \tilde{\sigma}^e_{a|x}. \tag{A.5}$$

Now, we finally consider that Eve also sends an additional degree of freedom which is read by the measuring device of Alice—an auxiliary classical 'flag' systems, which we label A′. This system has orthogonal states $|e\rangle$, for $e = 0, \ldots, m_{\text{A}} - 1$. This system will be read by Alice's measuring device, and, conditioned on the flag, the appropriate measurement will be made. We can thus now construct the complete strategy of Eve

$$\begin{aligned}\rho_{\text{ABE}} &= \sum_e P_{\text{E}}(e)|e\rangle\langle e|_{\text{A}'} \otimes \rho^e_{\text{AB}} \otimes |e\rangle\langle e|_{\text{E}} \\ M_{a|x} &= \sum_e |e\rangle\langle e|_{\text{A}'} \otimes M^e_{a|x} \\ M_e &= |e\rangle\langle e|_{\text{E}}.\end{aligned} \tag{A.6}$$

Clearly this defines a valid state and valid measurements, hence they satisfy the latter constraints of (A.2). Furthermore, by construction it also satisfies the first consistency constraint, which is straightforwardly verified.

In total, we thus conclude that the two optimization problems are equivalent, since the solution to either one implies a solution to the other, obtaining the same $P_{\text{guess}}(x^*)$. We thus focus on the problem (5) which is easier to solve, being an SDP optimization, linear in the optimization variables $\sigma^e_{a|x}$.

Appendix B. Derivation of the prepare-and-measure SDP

In this appendix we will show that the amount of randomness that can be certified in the prepare-and-measure scenario when Alice receives her share of the state through an untrusted channel, and does not trust her measuring device, is given by the SDP (6) in the main text.

Bob prepares a known bipartite state ρ_{AB} half of which is sent to Alice through the insecure quantum communication channel. Eve can intercept the state, and the most general operation she can perform (in the case

[9] Note that $P_{\text{E}}(e)$ is indeed independent of x, due to no-signalling, since $\sum_a \sigma^e_{a|x} = \sum_e \sigma^e_{a|x'}$ is independent of x.

that she is guessing only the outcome of a single measurement $x = x^*$) is a measurement with Kraus operators K_e, i.e. the POVM elements are $M_e = K_e^\dagger K_e$, and the state prepared by Eve after obtaining outcome e is

$$\rho_{\mathrm{AB}}^e = \frac{\left(K_e \otimes \mathbb{1}\right)\rho_{\mathrm{AB}}\left(K_e^\dagger \otimes \mathbb{1}\right)}{\mathrm{Tr}\left[K_e \rho_{\mathrm{A}} K_e^\dagger\right]} \tag{B.1}$$

which occurs with probability $P_{\mathrm{E}}(e) = \mathrm{Tr}[M_e \rho_{\mathrm{A}}]$. Eve will guess that the outcome of Alice's measurement is e. Eve now forwards the state onto Alice, and since she controls completely Alice's device, she will allow the device to perform the measurement $N_{a|x}^e$ when her outcome was e, and when Alice chooses to make measurement x (that is, Eve sends the classical information of which outcome she obtained along with the quantum state). Thus, the probability for Alice to obtain outcome a, given that she made measurement x and Eve obtained outcome e is given by

$$P_{\mathrm{A}}(a|x, e) = \frac{\mathrm{Tr}\left[N_{a|x}^e K_e \rho_{\mathrm{A}} K_e^\dagger\right]}{\mathrm{Tr}\left[K_e \rho_{\mathrm{A}} K_e^\dagger\right]}. \tag{B.2}$$

Putting everything together, we see therefore that the guessing probability is given by allowing Eve to optimize over all available strategies, and is given by

$$\begin{aligned} P_{\mathrm{guess}}\left(x^*\right) = \max_{K_e, N_{a|x}^e} & \sum_e \mathrm{Tr}\left[N_{a=e|x^*}^e K_e \rho_{\mathrm{A}} K_e^\dagger\right] \\ \text{subject to } & \sum_e \mathrm{Tr}_{\mathrm{A}}\left[\left(N_{a|x}^e \otimes \mathbb{1}\right)\left(K_e \otimes \mathbb{1}\right)\rho_{\mathrm{AB}}\left(K_e^\dagger \otimes \mathbb{1}\right)\right] = \sigma_{a|x}^{\mathrm{obs}} \quad \forall\ a, x \\ & \sum_a N_{a|x}^e = \mathbb{1} \qquad \forall\ e, x \\ & \sum_e K_e^\dagger K_e = \mathbb{1} \\ & N_{a|x}^e \succcurlyeq 0 \qquad \forall\ a, e, x. \end{aligned} \tag{B.3}$$

Currently, this optimization is not in the form of an SDP, due to the nonlinear nature of the objective function and the constraints. However, it can easily be written in the form of an SDP by introducing the new variable $M_{a|x}^e = K_e^\dagger N_{a|x}^e K_e$. The three final constraints on $N_{a|x}^e$ and K_e imply the following constraints on $M_{a|x}^e$,

$$\begin{aligned} \sum_a M_{a|x}^e = \sum_a M_{a|x'}^e, \ \forall\ e, x' \neq x, \\ \sum_{ae} M_{a|x}^e = \mathbb{1}, \ \forall\ x, \\ M_{a|x}^e \succcurlyeq 0, \quad \forall\ a, e, x. \end{aligned} \tag{B.4}$$

However, we can see that whenever we have a set of $M_{a|x}^e$ satisfying the above constraints, it implies that there exist $N_{a|x}^e$ and K_e satisfying the original constraints—i.e. the two sets are equivalent. To see this, we denote first $M_e = \sum_a M_{a|x}^e \succcurlyeq 0$ (which is independent of x), and therefore we can write $M_e = K_e^\dagger K_e$, for some K_e, which is always possible for a positive semi-definite operator. Moreover, since $\sum_{ae} M_{a|x}^e = \sum_e K_e^\dagger K_e = \mathbb{1}$, the second constraint is satisfied. Finally, defining $N_{a|x}^e = (K_e^\dagger)^{-1} M_{a|x}^e (K_e)^{-1} \succcurlyeq 0$ (using the pseudo-inverse when necessary), we also have that

$$\sum_a N_{a|x}^e = \left(K_e^\dagger\right)^{-1} M_e \left(K_e\right)^{-1} = \left(K_e^\dagger\right)^{-1} K_e^\dagger K_e \left(K_e\right)^{-1} = \mathbb{1}. \tag{B.5}$$

Thus, we can re-express the optimization problem (B.3) in the form of the following SDP

$$\begin{aligned} P_{\mathrm{guess}}\left(x^*\right) = \max_{M_{a|x}^e} & \sum_e \mathrm{Tr}\left[M_{a=e|x^*}^e \rho_{\mathrm{A}}\right] \\ \text{subject to } & \sum_e \mathrm{Tr}_{\mathrm{A}}\left[\left(M_{a|x}^e \otimes \mathbb{1}\right)\rho_{\mathrm{AB}}\right] = \sigma_{a|x}^{\mathrm{obs}} \qquad \forall\ a, x \\ & \sum_a M_{a|x}^e = \sum_a M_{a|x'}^e \qquad \forall\ e, x \neq x' \\ & \sum_{ae} M_{a|x}^e = \mathbb{1} \qquad \forall\ x, \\ & M_{a|x}^e \succcurlyeq 0 \qquad \forall\ a, e, x \end{aligned} \tag{B.6}$$

which is exactly the optimization problem given in the main text.

Appendix C. Deriving the dual of the SDP (5)

In this appendix we show the explicit form of the dual of the SDP (5), and explain why equation (9) is an equivalent form, which is easier to interpret.

As a reminder, the primal problem is given by

$$\begin{aligned} P_{\text{guess}}\left(x^*\right) = \max_{\sigma^e_{a|x}} \ & \sum_e \text{Tr}\left[\sigma^e_{a=e|x^*}\right] \\ \text{subject to} \quad & \sum_e \sigma^e_{a|x} = \sigma^{\text{obs}}_{a|x} \qquad \forall\ a,\ x \\ & \sum_a \sigma^e_{a|x} = \sum_a \sigma^e_{a|x^*} \quad \forall\ e,\ x \neq x^* \\ & \sigma^e_{a|x} \succcurlyeq 0 \qquad \forall\ a,\ x,\ e. \end{aligned} \tag{C.1}$$

Let us introduce dual variables $F_{a|x}, G^e_x$ and $H^e_{a|x}$, with respect to the first, second and third set of constraints respectively, and form the Lagrangian for this problem

$$\begin{aligned} \mathcal{L} = & \sum_e \text{Tr}\left[\sigma^e_{a=e|x^*}\right] + \sum_{ax} \text{Tr}\left[F_{a|x}\left(\sigma^{\text{obs}}_{a|x} - \sum_e \sigma^e_{a|x}\right)\right] \\ & + \sum_{aex} \text{Tr}\left[G^e_x\left(\sigma^e_{a|x} - \sigma^e_{a|x^*}\right)\right] + \sum_{aex} \text{Tr}\left[H^e_{a|x}\sigma^e_{a|x}\right]. \end{aligned} \tag{C.2}$$

After re-arranging, and grouping terms, this is equivalent to

$$\begin{aligned} \mathcal{L} = & \sum_{ax} \text{Tr}\left[F_{a|x}\sigma^{\text{obs}}_{a|x}\right] \\ & + \sum_{aex} \text{Tr}\left[\left(\delta_{a,e}\delta_{x,x^*}\mathbb{1} - F_{a|x} + G^e_x - \delta_{x,x^*}\sum_{x'} G^{e}_{x'} + H^e_{a|x}\right)\sigma^e_{a|x}\right]. \end{aligned} \tag{C.3}$$

This Lagrangian provides an upper bound on the primal objective as long as $H^e_{a|x} \succcurlyeq 0$. Moreover, it provides a non-trivial upper bound only when the inner bracket in the second line identically vanishes for each value of $a,\ e,\ x$. Thus, we arrive at the dual problem

$$\begin{aligned} P_{\text{guess}}\left(x^*\right) = \min_{F_{a|x}, G^e_x, H^e_{a|x}} \ & \sum_{ax} \text{Tr}\left[F_{a|x}\sigma^{\text{obs}}_{a|x}\right] \\ \text{subject to} \quad & \delta_{a,e}\delta_{x,x^*}\mathbb{1} - F_{a|x} + G^e_x - \delta_{x,x^*}\sum_{x'} G^{e}_{x'} + H^e_{a|x} = 0 \ \forall\ a,\ e,\ x \\ & H^e_{a|x} \succcurlyeq 0 \qquad \forall\ a,\ e,\ x. \end{aligned} \tag{C.4}$$

However, $H^e_{a|x}$ is playing the role of a slack variable, since it does not appear in the objective function, so we can finally simplify the dual to arrive at

$$\begin{aligned} P_{\text{guess}}\left(x^*\right) = \min_{F_{a|x}, G^e_x} \ & \sum_{ax} \text{Tr}\left[F_{a|x}\sigma^{\text{obs}}_{a|x}\right] \\ \text{subject to} \quad & F_{a|x} + \delta_{a,e}\delta_{x,x^*}\mathbb{1} - G^e_x - \delta_{x,x^*}\sum_{x'} G^{e}_{x'} \preccurlyeq 0 \qquad \forall\ a,\ e,\ x. \end{aligned} \tag{C.5}$$

The dual is easily seen to be strictly feasible, for example by taking $G^e_x = 0$ and $F_{a|x} = \alpha\mathbb{1}$ for $\alpha > 1$. Thus strong duality holds, and the optimal value of the dual is equal to the optimal value of the primal. In the form (C.5), the dual is seen manifestly to be an SDP, as expected. Finally, to understand the meaning of the constraint, we multiply by an arbitrary valid assemblage $\sigma_{a|x}$, and take the sum in a and x and the trace. We find

$$\sum_{ax} \text{Tr}\left[F_{a|x}\sigma_{a|x}\right] \geqslant \text{Tr}\left[\sigma_{e|x^*}\right] = P\left(e\,|x^*\right) \tag{C.6}$$

must hold for all e. Since this condition also holds for all valid assemblages, we see that the second constraint enforces that the value of the inequality is a uniform upper bound on the probability that any individual outcome occurs for the measurement x^*, independent of the assemblage. Hence, one sees immediately why this bounds the guessing probability.

Appendix D. Maximal randomness from all pure states

In this section we will show analytically that appropriate measurements on all partially entangled qudit states necessarily lead to 1 dit of randomness.

Consider first the partially entangled two-qubit state in Schmidt form, $|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$, for $\theta \in (0, \pi/4]$, and that Alice's two measurements are X and Z measurements respectively. The assemblage created for Bob is then

$$\begin{aligned}\sigma_{0|0} &= \frac{1}{2}\left|\uparrow_\theta\right\rangle\left\langle\uparrow_\theta\right|,\\ \sigma_{1|0} &= \frac{1}{2}\left|\uparrow_{-\theta}\right\rangle\left\langle\uparrow_{-\theta}\right|,\\ \sigma_{0|1} &= \cos^2\theta\,|0\rangle\langle 0|,\\ \sigma_{1|1} &= \sin^2\theta\,|1\rangle\langle 1|,\end{aligned} \tag{D.1}$$

where $|\uparrow_\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$. Crucially, each element of the assemblage is pure, i.e. each element is of the form $\sigma_{a|x} = P(a|x)\Pi_{a|x}$, where $\Pi_{a|x}$ is a one-dimensional projector. The purity of Bob's assemblage substantially constrains Eve's possible strategies, such that

$$\sigma^e_{a|x} = q(ae|x)\Pi_{a|x}, \tag{D.2}$$

where each $q(ae|x) \geqslant 0$. This says that Eve must prepare the same pure state for Bob in each instance, all she can vary is the probability of the two outcomes (which must still be positive). To be consistent with the observed assemblage, we must have that

$$\sum_e q(ae|x) = P(a|x). \tag{D.3}$$

The guessing probability also now becomes

$$P_{\rm g} = \sum_e \mathrm{tr}\left[\sigma^e_{a=e|0}\right] = q(00|0) + q(11|0). \tag{D.4}$$

Now, the no-signalling constraint says that $\sum_a \sigma^e_{a|0} = \sum_a \sigma^e_{a|1}$ for all e. Specifically, in the case at hand

$$q(0e|0)\Pi_{0|0} + q(1e|0)\Pi_{1|0} = q(0e|1)\Pi_{0|1} + q(1e|1)\Pi_{1|1}, \tag{D.5}$$

which must be true for all matrix elements. While the projectors on the right-hand side, corresponding to measurements of Z, are diagonal, the left-hand side, corresponding to X, are in general not diagonal. Thus, taking the trace with $|1\rangle\langle 0|$, we arrive at the condition

$$\cos\theta\,\sin\theta(q(0e|0) - q(1e|0)) = 0. \tag{D.6}$$

Since $\cos\theta\,\sin\theta \neq 0$ for $\theta \in (0, \pi/4]$, this implies that $q(0e|0) = q(1e|0)$. In particular, this says that $q(01|0) = q(11|0)$. However, to be consistent $q(00|0) + q(01|0) = p(0|0) = 1/2$, and thus we arrive at

$$1/2 = q(00|0) + q(01|0) = q(00|0) + q(11|0) = P_{\rm g}. \tag{D.7}$$

Thus, analytically it must be the case that $P_{\rm g} = 1/2$, and hence 1 bit of randomness is obtained by measuring X and Z on any partially entangled state of two qubits.

The above also extends to qudits; assuming that the state has Schmidt-rank d then 1 dit of randomness can always be obtained. Let us now write the state as

$$|\psi\rangle = \sum_{k=0}^{d-1}\sqrt{\lambda_k}\;|k\rangle|k\rangle, \tag{D.8}$$

where $\sum_k \lambda_k = 1$, and $\lambda_k > 0$. Alice's first measurement will now be in the Fourier transform basis, with eigenstates

$$\left|\tilde{a}\right\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{ak}\,|k\rangle \tag{D.9}$$

and $\omega = \mathrm{e}^{2\pi\mathrm{i}/d}$ the corresponding root of unity. Her second measurement will be in the Z basis with eigenstates $\{|a\rangle\}$. For Alice's first measurement she obtains each outcome with equal probability $P(a|0) = 1/d$, and prepares the pure states for Bob $\Pi_{a|0}$, given by

$$\Pi_{a|0} = \sum_{kl}\sqrt{\lambda_k\lambda_l}\,\omega^{a(l-k)}|k\rangle\langle l|. \tag{D.10}$$

For Alice's second measurement, she obtains outcome a with probability $P(a|1) = \lambda_a$, and prepares the state $\Pi_{a|1} = |a\rangle\langle a|$. As above, the purity of Bob's assemblage means that Eve is again forced to use strategies of the form $\sigma^e_{a|x} = q(ae|x)\Pi_{a|x}$. For consistency we still have $\sum_e q(ae|x) = P(a|x)$, for the guessing probability $P_{\rm g} = \sum_e q(ee|0)$, and from no-signalling $\sum_a q(ae|0)\Pi_{a|0} = \sum_a q(ae|1)\Pi_{a|1}$. Once again, the right-hand side is diagonal, and hence by looking at the off-diagonal matrix elements, i.e. by taking the trace with $|k\rangle\langle l|$, we find that

$$\sum_a q(ae|0)\sqrt{\lambda_k\lambda_l}\,\omega^{a(l-k)} = 0. \tag{D.11}$$

Since, by assumption of being Schmidt-rank d, none of the Schmidt coefficients vanish, we therefore must have that

$$\sum_a q(ae|0)\,\omega^{a(l-k)} = 0. \tag{D.12}$$

Considering only the elements with $k = 0$ (and $l = 1, \ldots, d-1$), along with the equation $\sum_a q(ae|0) = P(e)$, which says that Eve's probability to output e is just the marginal distribution, we notice that this set of equations, when combined, has the familiar form of a discrete Fourier transform (up to normalization):

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ 1 & \omega & \ldots & \omega^{d-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{d-1} & \ldots & \omega^{(d-1)^2} \end{bmatrix} \begin{bmatrix} q(0e|0) \\ q(1e|0) \\ \vdots \\ q(d-1,\,e|0) \end{bmatrix} = \begin{bmatrix} P(e) \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{D.13}$$

Thus, this equation is readily inverted, and we obtain as solution $q(ae|0) = P(e)/d$ for all $a,\ e$. In particular, this implies that Eve's guess is completely uncorrelated from Alice's, and her guessing probability is $P_{\mathrm{g}} = \sum_e q(ee|0) = \frac{1}{d}\sum_e P(e) = 1/d$. Thus 1 dit of randomness is obtained from Alice's measurement.

References

[1] Rarity J G, Owens P C M and Tapster P R 1994 *J. Mod. Opt.* **41** 2435
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lutkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[3] Bell J S 1964 *Physics* **1** 195
[4] Brunner N, Cavalcanti D, Pironio S, Scarani V and Wehner S 2014 *Rev. Mod. Phys.* **86** 419
[5] Colbeck R 2009 *PhD Thesis* University of Cambridge (arXiv: 0911.3814)
[6] Pironio S *et al* 2010 *Nature* **464** 1021
[7] Lydersen L *et al* 2010 *Nat. Photonics* **4** 686
[8] Gerhardt I *et al* 2011 *Nat. Commun.* **2** 349
[9] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Scarani V, Makarov V and Kurtsiefer C 2011 *Phys. Rev. Lett.* **107** 170404
[10] Schrodinger E 1935 *Proc. Camb. Phil. Soc.* **31** 555
[11] Wiseman H M, Jones S J and Doherty A C 2007 *Phys. Rev. Lett.* **98** 140402
[12] Quintino M T, Vértesi T, Cavalcanti D, Augusiak R, Demianowicz M, Acín A and Brunner N 2015 *Phys. Rev.* A **92** 032107
[13] Branciard C, Cavalcanti E G, Walborn S P, Scarani V and Wiseman H M 2012 *Phys. Rev.* A **85** 010301(R)
[14] Law Y Z, Thinh L P, Bancal J D and Scarani V 2014 *J. Phys. A: Math. Theor.* **47** 424028
[15] Ou Z Y, Pereira S F, Kimble H J and Peng K C 1992 *Phys. Rev. Lett.* **68** 3663
[16] Bowen W P, Schnabel R, Lam P K and Ralph T C 2003 *Phys. Rev. Lett.* **90** 043601
[17] Saunders D J, Jones S J, Wiseman H M and Pryde G J 2010 *Nat. Phys.* **6** 845
[18] Smith D-H *et al* 2012 *Nat. Commun.* **3** 625
[19] Bennet A J *et al* 2012 *Phys. Rev.* X **2** 031003
[20] Wittmann B *et al* 2012 *New J. Phys.* **14** 053030
[21] Händchen V *et al* 2012 *Nat. Photonics* **6** 598
[22] Armstrong S, Wang M, Teh R Y, Gong Q, He Q, Janousek J, Bachor H-A, Reid M D and Lam P K 2015 *Nat. Phys.* **11** 167–72
[23] Cavalcanti D, Skrzypczyk P, Aguilar G H, Nery R V, Souto Ribeiro P H and Walborn S P 2015 *Nat. Commun.* **6** 7941
[24] Li C-M, Chen K, Chen Y-N, Zhang Q, Chen Y-A and Pan J-W 2015 *Phys. Rev. Lett.* **115** 010402
[25] Nieto-Silleras O, Pironio S and Silman J 2014 *New J. Phys.* **16** 013035
[26] Bancal J D, Sheridan L and Scarani V 2014 *New J. Phys.* **16** 033011
[27] Bowles J, Quintino M T and Brunner N 2014 *Phys. Rev. Lett.* **112** 140407
[28] Li H-W, Pawlowski M, Yin Z-Q, Guo G-C and Han Z-F 2012 *Phys. Rev.* A **85** 052308
[29] Cavalcanti E G, Jones S J, Wiseman H M and Reid M D 2009 *Phys. Rev.* A **80** 032112
[30] Pusey M F 2013 *Phys. Rev.* A **88** 032313
[31] Quintino M T, Vértesi T and Brunner N 2014 *Phys. Rev. Lett.* **113** 160402
[32] Uola R, Moroder T and Gühne O 2014 *Phys. Rev. Lett.* **113** 160403
[33] Boyd S and Vandenberghe L 2004 *Convex Optimization* (Cambridge: Cambridge University Press)
[34] Gisin N 1989 *Helv. Phys. Acta* **62** 363371
Hughston P L, Jozsa R and Wootters W K 1993 *Phys. Lett.* A **183** 14
[35] Cavalcanti E G, Jones S, Wiseman H M and Reid M 2009 *Phys. Rev.* A **80** 032112
[36] Grant M and Boyd S 2013 *CVX: Matlab software for disciplined convex programming* version 2.0 beta http://cvxr.com/cvx
Blondel V *et al* (ed) 2008 Graph implementations for nonsmooth convex programs *Recent Advances in Learning and Control* (a tribute to M Vidyasagar) (*Lecture Notes in Control and Information Sciences*) (Berlin: Springer) pp 95–110
[37] Johnston N 2015 *QETLAB: A MATLAB toolbox for quantum entanglement* version 0.8 (http://www.qetlab.com)
[38] Acín A, Cavalcanti D, Passaro E, Pironio S and Skrzypczyk P 2015 arXiv:1505.00053
[39] Pusey M F 2015 *J. Opt. Soc. Am.* B **32** A56
[40] Acín A, Massar S and Pironio S 2012 *Phys. Rev. Lett.* **108** 100402